PRACTICAL EXPERIENCE IN TRANSFERRING PERSONAL DATA FROM THE EU TO HONG KONG

Webinar on the New Standard Contractual Clauses of the EU for Transfer of Personal Data from EU to Third Countries

September 2021

1 Introduction

Introduction

The General Data Protection Regulation (GDPR) regime on trans-boarder data transfers requires organisations to establish effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by European Union (EU) law

MORE THAN "TICK THE BOX" EXERCISE

It is not sufficient to simply adopt the Standard Contractual Clauses and consider that your data transfers are compliant with the GDPR

ONGOING EFFORTS

Ongoing efforts are required from both data importers and exporters. GDPR equivalent level of protection to that guaranteed within the EU must follow the data when it is transferred to and stored in Hong Kong

THE SCCs DO NOT OPERATE IN A VACUUM

The mechanisms and controls you put in place when transferring personal data from the EU to Hong Kong should form an integral part of your Privacy Management Programme.

When do the requirements for trans-boarder transfers apply?

WHAT CONSTITUTES A DATA TRANSFER?

And organisation is carrying out a transfer of personal data outside of the EU when it is **sending the personal data**, or **making it accessible**, to a receiver located in a country outside the EU and where the receiver is legally distinct from the organisation as it is a separate company, organisation or individual.

COMPANY WITHIN THE SAME CORPORATE GROUP

CLOUD SERVICE PROVIDER

STRATEGIC PARTNER

What parties can be considered as “Data Importers”?

Who is ‘Data Importer’ ?

Any person **other than**: -

a) the data subject;
b) a relevant person in the case of the data subject;
c) the data user;

Two types of Data Importers?

Data Processors

A processor is a natural or legal person, which processes personal data on behalf of Cathay. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the Cathay’s behalf.

Data Controllers

A controller determines the purposes and means of the processing, i.e. the why and how of the processing. The controller uses the data for it own purposes

2 Practical steps to adopting the SCCs and ensuring compliance

Practical Steps to ensuring compliance

To know what may be required for you (the data exporter) to be able to continue with or to conduct new transfers of personal data you must ensure that you are fully aware of your transfers*

Establishing an effective Privacy Impact Assessment process will help you to maintain your data registry up to date and to ensure that no new data transfers are carried before the required reviews are completed and necessary measures put in place

The principle of accountability requires continuous vigilance of the level of protection of personal data and ensuring that the third parties you are exporting personal data to comply with their commitments as stipulated in the clauses

* EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0

Data registry: Record of processing activities

Record providing **in-depth understanding of personal data handling practices** including what personal data is collected and how is it used

A document with inventory and analysis purposes, which reflect the reality of our personal data processing and help us identify:

- The **actors involved** (controller, processors, representative, joint controller, etc.) in the data processing;
- The **categories of data processed/transferred** (including sensitive data);
- The **purpose of the processing/transfer**
- **Who has access** and who are the recipients of the personal data;
- **Location of storage/ transfer**
- **Retention of the personal** data;
- The **technical and organizational measures** implemented.

Why is it important ?

Knowing your personal data is the fundamental step to data protection compliance and the importance of having a robust personal data inventory or a record of processing activities is amplified when it comes to ensuring compliance with the GDPR requirements on international data transfers

1. **It will help you to complete ANNEX I OF THE SCCs requiring to clearly distinguish the information applicable to each transfer or category of transfers**

2. **Knowing in which jurisdictions your organization is transferring personal data is fundamental to required under the Schrems II decision CARRYING OUT THE DATA TRANSFER IMPACT ASSESSMENT**

3. **Will help you document the relevant technical and organisational MEASURES FOR PROTECTING THE DATA AS WELL AS ANY SUPPLEMENTAL TRANSFER TOOLS**

Privacy Impact Assessment

What is Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a systematic assessment of a project that identifies the impact that the project might have on the privacy of customers and employees and sets out recommendations for managing, minimising or eliminating that impact

What question do you need to consider when carrying out PIA for international data transfers?

DETAILED DESCRIPTION OF THE DATA FLOW

- Categories of data subjects whose personal data is transferred
- Categories of personal data transferred
- Sensitive data transferred and applied restrictions or safeguards
- The frequency of the transfer
- Purpose(s) of the data transfer and further processing
- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
- Transfers to (sub-) processors

THIRD COUNTRY ASSESSMENT

- Is there a robust privacy law?
- Is there an independent supervisory authority?
- Are government authorities allowed access to personal data held by companies for surveillance purposes?
- Is there any oversight mechanism?
- Are there any legal remedies available to individuals and organizations?

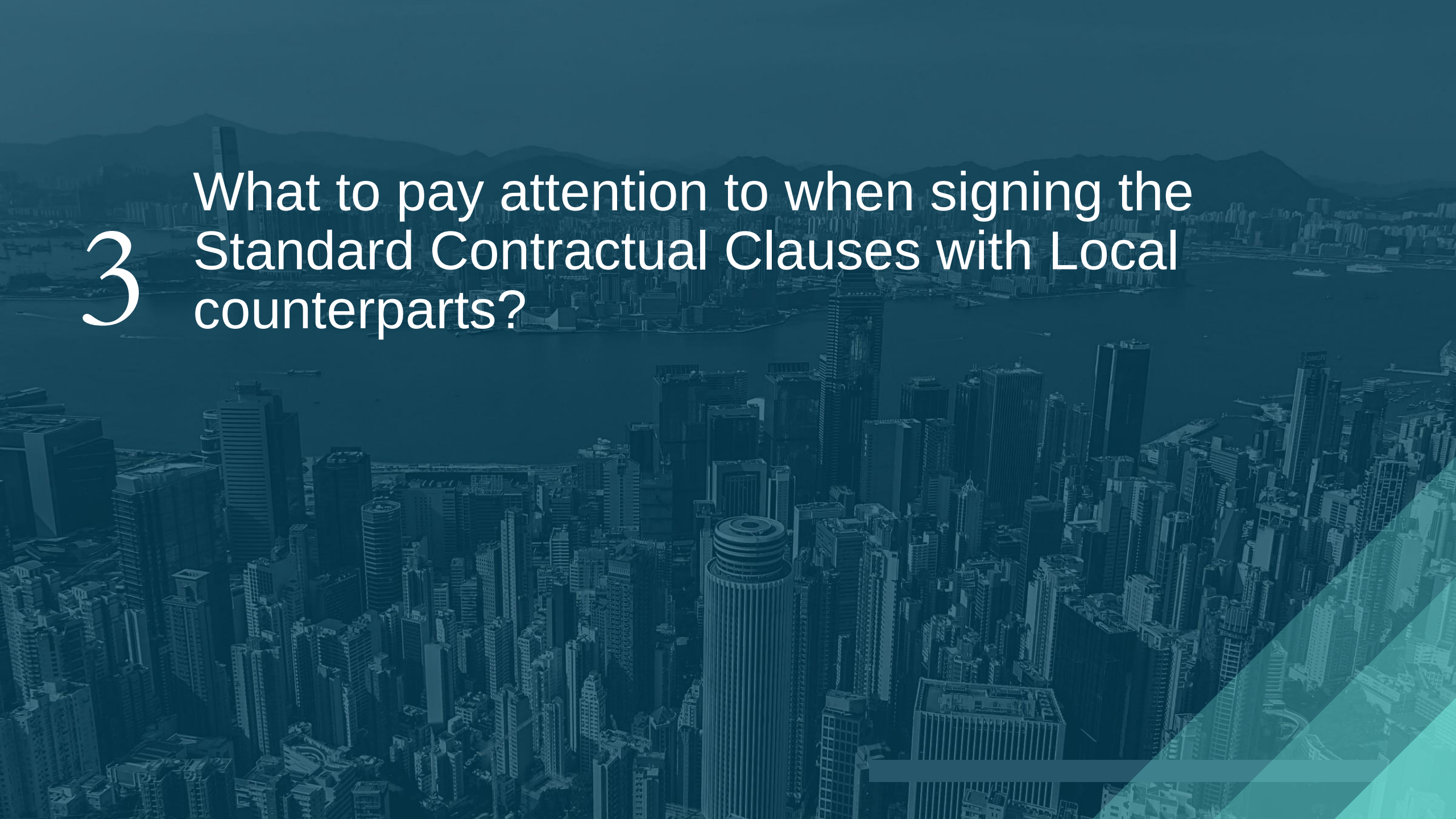
TECHNICAL AND ORGANIZATIONAL MEASURES & SUPPLEMENTARY MEASURES

- Pseudonymisation and encryption
- Ensuring the ability to restore the availability and access to personal data in a timely manner
- Processes for regularly testing
- User identification and authorisation
- Protection of data during transmission
- Protection of data during storage
- Ensuring physical security of locations at which personal data are processed
- Ensuring events logging
- Internal IT and IT security governance and management

Ongoing Monitoring

The principle of accountability requires continuous vigilance of the level of protection of personal data and ensuring that the third parties you are exporting personal data to comply with their commitments as stipulated in the clauses.

1. **ENSURING THAT THE DATA IMPORTER'S HANDLING PRACTICES MEET IT'S CONTRACTUAL COMMITMENTS**
2. **IDENTIFYING AREAS OF IMPROVEMENT**
3. **DEMONSTRATE COMPLIANCE IN LINE WITH THE ACCOUNTABLY PRINCIPLE**



3 What to pay attention to when signing the Standard Contractual Clauses with Local counterparts?

INVARIABILITY

Standard Contractual Clauses are considered appropriate safeguards, with respect to data transfers, ***provided they are not modified***

OBLIGATIONS OF THE DATA IMPORTERS

The SCCs require data importers to introduce robust technical and organizational measures and you need to make sure that they are **capable to comply with them**

Pay special attention to Clause 14 which requires the Data Importers to have in-depth understanding of the local laws and practices affecting compliance with the Clauses

APPLICABLE LAW AND JURISDICTION

The new clauses require the contracting parties to choose as applicable law the law of one of the EU Member States, provided such law allows for third party beneficiary rights

THANK YOU!